UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,126	12/04/2001	Andrew Duke	10001-30614	8033

2574 7590 06/29/2004

JENNER & BLOCK, LLP
ONE IBM PLAZA
CHICAGO, IL 60611

EXAMINER	
EHICHIOYA, FRED I	

ART UNIT	PAPER NUMBER
2172	5

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/004,126	DUKE ET AL.
	Examiner	Art Unit
	Fred I. Ehichioya	2172

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 5 - 15, 17 - 19* is/are rejected.

7)☒ Claim(s) *2-4* is/are objected to.

8)☒ Claim(s) *1 - 15, 17 - 19 and 16* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 - 19 are pending in this application.

Information Disclosure Statement

2. The reference cited in the information disclosure statement, IDS- Form 1449 has been considered by the examiner.

Election/Restrictions

3. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1 - 15 and 17 - 19, drawn to storing and updating information in a network, classified in class 707, subclass 200.

II. Claim 16, drawn to encryption of messages, classified in class 713, subclass 201.

The inventions are distinct, each from the other because of the following reasons:

4. Inventions listed as Group I and Group II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention has separate utility as follows:

Group I: storing and updating information in a network.

Group II: Encryption of messages.

See MPEP § 806.05(d).

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

6. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

7. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

8. During a telephone conversation with Michael Bell, Attorney for the Applicant, registration Number 39,604 on June 25, 2004 a provisional election was made without traverse to prosecute the invention of Group I, claims 1 - 15 and 17 - 19. Affirmation of this election must be made by applicant in replying to this Office action. Claim 16 withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

9. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 5, 6, 8 – 15, and 17 - 19 are rejected under 35 U.S.C 102(b) as been anticipated by Non-Patent Literature document by D. Wallner et al (hereinafter "Wallner"), Key Management For Multicast: Issues and Architectures", June 1999, The Internet Society.

Regarding claim 1, Wallner teaches a method for storing and updating information in a network having *n* hierarchical levels, said method comprising the steps of:

defining a root node positioned in a first of said levels, said root node having no parent node and at least one child node (see Fig. 2, where the root node is Key O with no parent node and at least Key M and Key N as child nodes);

defining at least two leaf nodes positioned in an nth of said levels, each of said leaf nodes having a parent node and no child node (see Fig. 2, where Key M and Key N are leaf node and n level is first level);

defining a corresponding path between each of said at least two leaf nodes and said root node (see Fig.2, where each of said at least two leaf nodes

and said root node are Key M – Key O or Key N – Key O);

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child node of said non-leaf node (see Fig. 2 and pages 14 and 15); and

providing each leaf node with a related set of keys wherein said related set of keys includes each key associated with each non-leaf node on said corresponding path from said leaf node to said root node (see Fig. 2, section 5.4.1 pages 14 and 15).

Regarding claim 5, Wallner teaches each non-leaf node is associated with more than two child nodes (see Fig. 2, where Key I is a non-leaf node associated with Key A and Key B).

Regarding claim 6, Wallner teaches each non-leaf node is associated with the same number of child nodes (see Fig. 2, Key I and Key J are non-leaf nodes associated with Key A and Key B and key C and Key D respectively).

Regarding claim 8, Wallner teaches aim 1 further comprising the step of identifying a specific one of said leaf nodes as a compromised leaf node (see page 17, paragraph 1).

Regarding claim 9, Wallner teaches the step of removing at least a portion of said path between said compromised leaf node and said root node (see page 14, paragraph 4).

Regarding claims 10 and 14, Wallner teaches the step of marking a key in said set of keys related to said compromised leaf node as a compromised key (see pages 7 and 8, section 5.1).

Regarding claim 11, Wallner teaches the step of sending a message from said root node to a non-compromised leaf node using a key that has not been marked as a compromised key (see page 15, paragraph 2).

Regarding claim 12, Wallner teaches the step of identifying each of one or more specific leaf nodes as a compromised leaf node (see page 17, paragraph 1).

Regarding claim 13, Wallner teaches the step of removing at least a portion of said path between each of said one or more compromised leaf nodes and said root node (see page 12, section 5.4 and #1).

Regarding claim 15, Wallner teaches the step of sending a message from said root node to a non-compromised leaf node using a key that has not been marked as a compromised key (see page 19, section 5.4.2.4 paragraphs 1 and 2).

Regarding claim 17, Wallner teaches a system for storing and updating information in a network having a plurality of hierarchical levels, comprising:

a root node associated with a highest of said levels, said root node having at least two child nodes and no parent node (see Fig. 2, where the root node is Key O with no parent node and at least Key M and Key N as child nodes);

at least two leaf nodes associated with a lowest of said levels, each of said leaf nodes having a parent node and no child node (see Fig.2, Key a and Key B are two leaf nodes associated with a lowest of said levels having parent node Key I but no child node);

a corresponding path between each of said at least two leaf nodes and said root node (see Fig. 2, corresponding path between each of said at least two leaf nodes and said root node are: Key A – Key I – Key M – Key O or Key B – Key I – Key M – Key O); and

at least one key associated with each node associated with a level higher than said lowest level, each of said at least one key corresponding to a specific child or specific children of said node associated with a level higher than said lowest level, wherein each of said leaf nodes includes each key associated with each non-leaf node on said corresponding path from said leaf node to said root node (See Fig.2, Key M is associated with each node associated with a level higher than said lowest level (Key O) and corresponds to children Key I and Key J; 1, 2, 3 and 4 are leaf includes each key associated with

each non-leaf node on said corresponding path from said leaf node to said root

node Key O).

Regarding claim 19, Wallner teaches said root node may send a message to at least one leaf node (see page 14, paragraphs 1 and 2).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 7 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wallner in view of Non-Patent Literature document by David A. McGrew et al (hereinafter "McGrew"), Key Establishment in Large Dynamic Group Using One-Way Function Trees, May 20, 1998, Cryptographic Technologies Group, Glenwood, MD.

Regarding claim 7, Wallner does not explicitly teach internal node

McGrew teaches the step of defining an internal node positioned on said corresponding path between said root node and a first of said leaf nodes, said internal node being associated with a hierarchical level between said first level and said nth level (see page 3, section 3.1).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine teaching of McGrew with the teaching of Wallner wherein the each member's knowledge about the current state of the key tree is limited. The motivation is that the invention creates a system where group members communicate with privacy and or authentication.

Regarding claim 18, McGrew teaches at least one internal node on said corresponding path between each of said leaf nodes and said root node, each of said internal nodes having a parent node and at least one child node, each of said internal nodes associated with a further one of said plurality of levels (see pages 3 – 5, sections 3.1, 3.2, 3.3, and 4).

Claim Objections

13. Claims 2, 3 and 4 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: As to claim 2, the prior art of record does not teach or fairly suggest wherein said corresponding set of keys associated with each non-leaf node includes $2^m - 1$ keys where *m* is the maximum number of child nodes that may be associated with each non-leaf node; As to claim 3, the prior art of record does not teach or fairly suggest wherein said corresponding set of keys associated with each non-leaf node includes $2^m - 2$ keys where *m* is the maximum number of child nodes that may be associated with each non-leaf node; As to claim 4, the prior art of record does not teach or fairly suggest wherein said related set of keys provided to each leaf node includes $(n-1)*(2^m - 1)$ keys where *m* is the maximum number of child nodes that may be associated with each non-leaf node.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fred I. Ehichioya whose telephone number is 703-305-8039. The examiner can normally be reached on M - F 8:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fred I. Ehichioya
Examiner
Art Unit 2172
June 27, 2004

SHAHID ALAM
PRIMARY EXAMINER